REMARKS/ARGUMENTS

The Applicant has added a new paragraph to page 1 of the specification entitled "Cross Reference to Related Application". The Applicant submits that this amendment introduces no new matter.

The Examiner rejects claims 1 – 27 under 35 USC 103(a) as being unpatentable over US Patent No. 4,710,613 (Shigenaga) in view of US Patent No. 5,923,759 (Lee). The applicant has enacted further amendments to the independent claims 1 and 14 and submits the following remarks for the Examiner's consideration. It is respectfully submitted that the amendments together with the clarifying remarks traverse the rejection under 35 USC 103(a).

Independent claims 1 and 14 have been amended to differentiate the claimed invention from Shigenaga and Lee. Claims 1 and 14 now recite that the untrusted authentication chip is contained within a consumable and the trusted authentication chip is contained within a consuming device.

Support for this amendment is found, for example, at page 4, lines 11 – 17 of the present specification. Further support can be found, for example, in the discussion of consumables at page 41, line 6 to page 42, line 28.

A consumable, by it's definition, in intended to be used up and then replaced. A consuming device is the device that consumes the consumable. Currently amended claims 1 and 14 are now directed to a validation protocol and a validation system, respectively, for use in conjunction with a consuming device and a consumable.

Shigenaga

Referring to Shigenaga, there is only disclosure of an IC card used in conjunction with an IC card terminal. Used in conjunction with a Personal Identification Number (PIN), Shigenaga discloses a system of authorisation for use of the IC card.

At page 5 of the Office Action, the Examiner, in referring to claims 6 – 7, considers that Shigenaga discloses a system in which the IC card is a consumable. It is respectfully submitted that such an interpretation in inconsistent with the normal English meaning of the term "consumable". The IC card is not consumed by the IC card terminal (which is not a consuming device).

In the present invention, a consumable is a device which needs to be replaced, for example, as disclosed at page 4 of the specification, a print roll, an ink cartridge, a toner cartridge, etc.. The applicant desires to make clear that the term consumable should not be considered to be limited to only these devices, however, the applicant asserts that it is clear that a consumable is not an IC card.

Furthermore, it is respectfully submitted that one of ordinary skill in the art is not taught how to produce the presently claimed invention, as defined in claim 1 or 14 in light of Shigenaga. There is no teaching, suggestion or motivation found in Shigenaga, or other prior art documents of record, that would motivate one of ordinary skill in the art to modify the teachings of Shigenaga for use in a consumable and a consuming device. Shigenaga is directed to confirming authorization of a user to use an IC card. Shigenaga is not concerned with the long standing problems associated with authenticating a consumable to prevent inferior refill operations or clone manufacturing of consumables. Existing solutions to the ongoing problem of authenticating consumables have typically relied on unique packaging or physical interconnections which does not teach or suggest to one of ordinary skill in the art that the disclosures in Shigenaga would find application in the problem of authenticating consumables.

Furthermore, independent claims 1 and 14 have been amended for clarity. Previous use of the term "second decrypted outcome" has been replaced by "first decrypted outcome", previous use of the term "third encrypted outcome" has been replaced with the term "second encrypted outcome" which the applicant submits better clarifies the invention as previously a "first decrypted outcome" had not been recited in the claims.

Lee

The Examiner relies on column 6, line 37 – 67 of Lee as reciting features of claim 1. However, it is respectfully submitted that the combination of Shigenaga and Lee does not teach or suggest currently amended claim 1 or 14. Referring to claim 1, a required step is "applying, in the untrusted authentication chip an asymmetric encrypt function to the first decrypted outcome together with an original data message read from the untrusted authentication chip using the second secret key to produce a second encrypted outcome". In Lee such a step does not occur. In Lee there are two separate authentication processes occurring independently, being authenticate card routine 300 and authenticate host routine 310. Under routine 300, processor 122 generates a random number and transmits it to the card. The card receives the random number, encrypts the random number using an internal key stored in the card and returns the encrypted random number to processor 122. Processor 122 then decrypts the number based upon the same algorithm and an identifying key stored in memory 126. Processor 122 then compares the original random number and the decrypted random number.

Separately, under routine 310, the card generates a random number and transmits it to processor 122 which receives the random number, encrypts the random number using an identifying key stored in memory 126 and returns the encrypted random number to the card. The card then decrypts the received number from processor 122 and compares the original random number with the decrypted random number.

This merely describes a similar process either occurring in the card or in processor 122. This does not describe the step recited in claim 1. In claim 1, it is the first decrypted outcome <u>together with</u> an original data message that is used to produce a second encrypted outcome. In Lee, there is only disclosed a simple generation of a random number, encryption of the random number, and decryption of the encrypted random number in another device, whether being the processor or the card. Lee does not disclose generation of a random number, encryption of the random number, decryption of the random number and further encryption of the random number together with an original data message. It should also be noted that the original data message recited in present claim 1 is not an "internal key" as found in Lee at column 6, line 43, which refers to a key for encryption.

In present claim 1, it is the <u>second encrypted outcome</u> together with the original data message which is passed to the trusted authentication chip. Hence, in this step the original data message is passed to the trusted authentication chip twice, as the original data message and also appended to the first decrypted outcome which has been further encrypted to produce the second encrypted outcome. Such a step is not disclosed or suggested in Shigenaga or Lee, either individually or in combination.

In present claim 1, the comparison is made between the decrypted random number and the decrypted data message with the original random number and the received original data message without knowledge of the second secret key. In contrast, Lee merely discloses comparison of a decrypted random number with an original random number, which is already disclosed in Shigenaga.

Furthermore, Lee does not disclose that the second secret key should remain secret from the trusted authentication chip. Indeed, at column 7, line 9, Lee states that known algorithms may be used, including symmetrical algorithms. This highlights a significant difference between the process in Lee and the protocol defined in claim 1 that cannot operate with a symmetrical encryption/decryption algorithm.

Similar remarks apply to currently amended claim 14 directed to a consumable authentication system. Also, it is submitted that dependent claims 2 – 6, 8, 9, 11 – 13, 15 – 19, 21, 22 and 24 – 27 define patentable subject matter as they incorporate all the features of either independent claim 1 or 14.

It is respectfully submitted that all of the Examiner's objections have been successfully traversed. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application is courteously solicited.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

C/o:	Silverbrook Research Pty Ltd 393 Darling Street Balmain NSW 2041, Australia
Email:	kia.silverbrook@silverbrookresearch.com
Telephone:	+612 9818 6633
Facsimile:	+61 2 9555 7762